The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game

Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi

Motivation: The security of any system is a direct consequence of stakeholders' decisions regarding security requirements and their relative prioritisation. Such decisions are taken with varying degrees of expertise in security. In some organisations – particularly those with resources – these are the preserve of computer (or information) security teams. In others – typically smaller organisations – the computing services team may be charged with the responsibility. Often managers have a role to play as guardians of business targets and goals. Be it common workplace practices or strategic decision making, security decisions underpin not only the initial security requirements and their prioritisation but also the adaptation and evolution of these requirements as new business or security contexts arise.

However, little is currently understood about how these various demographics approach cyber security decisions and the strategies and approaches that underpin those decisions. What are the typical decision patterns, if any, the consequences of such patterns and their impact (positive or negative) on the security of the system in question? Nor is there any substantial understanding of how the strategies and decision patterns of these different groups contrast. Is security expertise necessarily an advantage when making security decisions in a given context? Answers to these questions are key to understanding the "how" and "why" behind security decision processes.

The Game: In this talk[1], we present a tabletop game – Decisions and Disruptions (D-D)[2] – as a means to investigate these very questions. The game tasks a group of players with managing the security of a small utility company while facing a variety of threats. The game provides a requirements sandbox in which players can experiment with threats, learn about decision making and its consequences, and reflect on their own perception of risk. The game is intentionally kept short – 2 hours – and simple enough to be played without prior training. A cyber-physical infrastructure, depicted through a Lego® board, makes the game easy to understand and accessible to players from varying backgrounds and security expertise, without being too trivial a setting for security experts.

Key insights: We played D-D with 43 players divided into homogeneous groups (group sizes of 2-6 players): 4 groups of security experts, 4 groups of non-technical managers and 4 groups of general computer scientists. Such observations should, of course, not be generalised, however, the substantial sample size enables in-depth qualitative analysis. Our analysis reveals a number of novel insights regarding security decisions of our three demographics:

- ***Strategies:*** Security experts had a strong interest in advanced technological solutions and tended to neglect intelligence gathering, to their own detriment: some security expert teams achieved poor results in the game. Managers, too, were technology-driven and focused on data protection while neglecting human factors more than other groups. Computer scientists tended to balance human factors and intelligence gathering with technical solutions, and achieved the best results of the three demographics.
- ***Decision Processes:*** Technical experience significantly changes the way players think. Teams with little technical experience had shallow, intuition-driven discussions with few concrete arguments. Technical teams, and the most experienced in particular, had much richer debates, driven by concrete scenarios, anecdotes from experience, and procedural thinking. Security experts showed a high confidence in their decisions – despite some of them having bad consequences – while the other groups tended to doubt their own skills – even when they were playing good games.
- ***Patterns:*** A number of characteristic plays could be identified, some good (balance between priorities, open-mindedness, and adapting strategies based on inputs that challenge one's pre-conceptions), some bad (excessive focus on particular issues, confidence in charismatic leaders), some ugly ("tunnel vision" syndrome by over-confident players). We document and discuss these patterns, showing the virtue of the positive ones, discouraging the negative ones, and inviting the readers to do their own introspection.

Conclusion: D-D complements existing work on gamification as a means to improve security awareness, education, and training. Beyond the analysis of the security decisions of the three demographics, there is a definite educational and awareness-raising aspect to D-D (as noted consistently by players in all our subject groups). Game boxes will be brought to the conference for demonstration purposes, and the audience will be invited to experiment with D-D themselves, make their own decisions, and reflect on their own perception of security.

[1]Original journal paper: S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, and S. A. Naqvi. The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. IEEE TSE, 2017.

[2]Game rules available at: http://decisions-disruptions.org.